UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/627,117	07/24/2003	Peter Dam Neilsen	857.0019.U1(US)	3924

29683 7590 06/16/2009
HARRINGTON & SMITH, PC
4 RESEARCH DRIVE, Suite 202
SHELTON, CT 06484-6212

EXAMINER	
TIMBLIN, ROBERT M	

ART UNIT	PAPER NUMBER
2167	

MAIL DATE	DELIVERY MODE
06/16/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/627,117	NEILSEN ET AL.	
	Examiner	Art Unit	
	ROBERT TIMBLIN	2167	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 March 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2,3,5-9,20,23,33,34,36-40,46 and 52-64* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2,3,5-9,20,23,33,34,36-40,46 and 52-64* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action corresponds to application 10/627,117 which was filed 7/24/2003. Claims 2, 3, 5-9, 20, 23, 33-34, 36-40, 46, and 52-64 are pending.

Specification

The abstract of the disclosure is objected to because "Fig. 2" found on the abstract sheet should be removed. Correction is required. See MPEP § 608.01(b).

Response to Amendment

In the reply filed 3/16/2009, Applicant amends claims 2, 3, 5-9, 20, 23, 33, 34, 36, 37-40, 46, 52-53, 56, 58 and 60. Claims 61-64 have been newly added.

Claim Objections

Examiner thanks Applicant for the correcting amendments that change the leading "A" to "The" in the depending claims 2-3, 5-9, 23, 34, 36-40, 52. The objections under this issue have been removed.

Examiner thanks Applicant for the correcting amendment to Claim 46. The objection has been removed.

Upon further examination, Claim 58 is objected to for concluding with two periods. One of the periods should be deleted to correct this supposed typographical error.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 2, 3, 6, 9, 20, 23, 33, 34, 37, 40, 46, 52-57, and 60 are rejected under 35 U.S.C. 102(e) as being taught by Meffert et al. ('Meffert' hereafter) who filed U.S. Patent Application 2003/0037261.

With respect to claim 2, The method as claimed in claim 23, further comprising subsequent to step d), requesting entry of a first password to enable the further display of the first data assemblage and subsequent to step f), requesting entry of the first password to enable the further display of the second data assemblage does not restrict the data being displayed for the first time using the password (0120; "the trial level access permits the user is permitted to listen to the song/track once and thereafter is precluded from listening without again obtaining the proper authorization").

With respect to claim 3, The method as claimed in claim 23, further comprising, before step a), wirelessly receiving the first data assemblage at the hand portable device (0045) and before step e), wirelessly receiving the second data assemblage at the hand portable device (0098).

With respect to claim 6, The method as claimed in claim 5, further comprising user specification of the at least one defined type (fig. 3 and 4A).

With respect to claim 9, The method as claimed in claim 23 wherein at least one of the first data assemblage and the second data assemblage is created in the device (drawing reference 2001 and 0091).

With respect to claim 20, A method comprising:

a) storing (0041, 0080; e.g. downloading content) a plurality of data assemblages (0037; e.g. "...system and method that sends data such as documents, email, music files, XML content, etc. (hereinafter "content)) in a hand portable device (0041, 0130);

a1) automatically discriminating (0046; e.g. therein it is described that encrypted content in a wrapper is acted upon for content control) between at least one defined type of data assemblages that contain user personal data (0116; wherein emails and music files represent personal data) and other types of data assemblages that do not

contain user personal data (0100: e.g. browser content; 0109: e.g. downloaded applets; 0119: e.g. notifying messages);

b) storing at least one data attribute (0122; e.g. "songs/tracks are stored with certificates and are ready for sales..." and 0126; e.g. "the trial key that is preferable attached to the content") for each (0123; "...certificate generated per song...") of a plurality of first data assemblages (0037; e.g. "...system and method that sends data such as documents, email, music files, XML content, etc. (hereinafter "content)) that contain the user personal data, the data attribute (0122; e.g. "songs/tracks are stored with certificates and are ready for sales..." and 0126; e.g. "the trial key that is preferable attached to the content" as well as DRM information, 0125) indicative of a first display (0120) of a corresponding first data assemblage in the device (0041, 0130);

c) displaying for a first time (0049, 0095, 0126; e.g. a "trial play" i.e. single use or viewing one time only) in the hand portable device (0041, 0130) a first data assemblage (0126) of the plurality of first data assemblages (0037; e.g. "...system and method that sends data such as documents, email, music files, XML content, etc. (hereinafter "content)) without regard to a first security mechanism (0120; "the trial level access permits the user is permitted to listen to the song/track once and thereafter is precluded from listening"), and responsive to the displaying for the first time (0126; e.g. a "trial play" i.e. single use) automatically changing the data attribute (0120, 0127) of the displayed one of the first data assemblage from a first type to a second type (0031, 0126-0127; e.g. therein it is described that a file subject to a trial use is able to be

accessed and thereafter not entitled to further playing. As such, an attribute for viewing is described to be changed after expiration of the trial period/use); and

d) in response to changing the data attribute type (0031, 0126-0127) of step c), automatically restricting further display (0120, 0127) of the first data assemblage (0126) using the first security mechanism (0120; "the trial level access permits the user is permitted to listen to the song/track once and thereafter is precluded from listening" without again obtaining the proper authorization).

With respect to claim 23, The method as claimed in claim 20, further comprising, subsequent to step d):

e) displaying for a first time (0126; e.g. a "trial play" i.e. single use) in the hand portable device a second data assemblage (0123 "per song" indicates the method applicable to each [additional/second] file) of the plurality of first data assemblages that contain the user personal data (0037; e.g. "...system and method that sends data such as documents, email, music files, XML content, etc. (hereinafter "content)) without regard to the first security mechanism, and responsive to the displaying for the first time (0126; e.g. a "trial play" i.e. single use) the second data assemblage (0123 "per song" indicates the method applicable to each [additional/second] file) automatically changing the data attribute of the second data assemblage from the first type to the second type; and

f) in response to changing the data attribute of step e), automatically restricting further display (0120, 0127) of the second data assemblage using the first security

mechanism (0120; "the trial level access permits the user is permitted to listen to the song/track once and thereafter is precluded from listening").

With respect to claim 33, A hand-portable device comprising:

an input configured to receive of a password (0092, drawing reference 900);

a memory (0068) configured to store data (0037; content);

a display (0041) configured to display means for displaying the data (0037; content); and

a processor (0086) configured to automatically discriminate (0046; e.g. therein it is described that encrypted content in a wrapper is acted upon for content control) between at least one defined type of data assemblages that contain user personal data (0116; wherein emails and music formats represent personal data) and other types of data assemblages that do not contain user personal data (0100: e.g. browser content; 0109: e.g. downloaded applets; 0119: e.g. notifying messages), said processor further configured to detect that certain data (0037; content) has been displayed for a first time (0079: e.g. "a sender may elect to have content viewed only once and/or set authentication options for recipient whereby the local agent on the recipient's computer will permit viewing of the content one time only"; 0126; e.g. a "trial play" i.e. single use) at the display means and automatically responsive to detecting that certain data has been displayed for the first time to restrict subsequent (0120, 0127) display of certain data (0037; content) using a first security mechanism involving the password (0120; e.g. "...is precluded from listening without again obtaining the proper authorization." and

0138), wherein the processor (0086) does not restrict the data being displayed for the first time using the password (0120; "the trial level access permits the user is permitted to listen to the song/track once and thereafter is precluded from listening").

With respect to claim 34, The hand-portable device as claimed in claim 33, further comprising a transceiver configured to wirelessly receive means for wirelessly receiving the data assemblages that contain user personal data at the hand portable device (figure 11, customer site).

With respect to claim 37, The hand-portable device as claimed in claim 33, wherein said processor is further configured with the input to enable a user of the device to specify the at least one defined type (fig. 3, 4A).

With respect to claim 40, The hand-portable device as claimed in claim 33, wherein the data assemblages that contain user personal data are created in the device (drawing reference 2001 and 0091).

With respect to claim 46, A memory storing a computer program and readable by a processor for enabling a mobile telephone to perform actions directed to restricting access to a first data assemblage, the actions comprising:

a) storing (0041, 0080; e.g. downloading content) a plurality of data assemblages (0037; e.g. "...system and method that sends data such as documents, email, music files, XML content, etc. (hereinafter "content)) in a mobile telephone (0131);

a1) automatically discriminating (0046; e.g. therein it is described that encrypted content in a wrapper is acted upon for content control) between at least one defined type of data assemblages that contain user personal data (0116; wherein emails and music formats represent personal data) and other types of data assemblages that do not contain user personal data (0100: e.g. browser content; 0104: e.g. downloaded applets; 0119: e.g. notifying messages);

b) storing at least one data attribute (0122; e.g. "songs/tracks are stored with certificates and are ready for sales..." and 0126; e.g. "the trial key that is preferable attached to the content") for each (0123; "...certificate generated per song...") for each of a plurality of first data assemblages (0037; e.g. "...system and method that sends data such as documents, email, music files, XML content, etc. (hereinafter "content))that contain the user personal data, the data attribute indicative of a first display (0095, 0120) of a corresponding first data assemblage in the mobile telephone (0131);

c) displaying for a first time (0049, 0095, 0126; e.g. a "trial play" i.e. single use or viewing one time only) in the mobile telephone (0131) a first data assemblage of the plurality of first data assemblages without regard to a first security mechanism (0120; "the trial level access permits the user is permitted to listen to the song/track once and thereafter is precluded from listening"), and responsive to the displaying for the first time (0126; e.g. a "trial play" i.e. single use) automatically changing the data attribute (0120,

0127) of the displayed one of the first data assemblage from a first type to a second type (0031, 0126-0127; e.g. therein it is described that a file subject to a trial use is able to be accessed and thereafter not entitled to further playing. As such, an attribute for viewing is described to be changed after expiration of the trial period/use); and

d) in response to changing the data attribute (0031, 0126-0127) of step c), automatically restricting further display of the first data assemblage in the mobile telephone (0131) using the first security mechanism (0120; "the trial level access permits the user is permitted to listen to the song/track once and thereafter is precluded from listening" without again obtaining the proper authorization).

With respect to claim 52, The hand portable device as claimed in claim 33, wherein:

the memory is further configured to store a second data assemblage, that also contains user personal data (0123 "per song" indicates the method applicable to each [additional/second] file), the display is further configured to enable a user to display the second data assemblage that also contains user personal data (0123 "per song" indicates the method applicable to each [additional/second] file), and the processor access control means is further configured arranged to detect that the second data assemblage that also contains user personal data has been displayed for a first time at the display and automatically responsive to detecting that the second data assemblage that also contains user personal data (0123 "per song" indicates the method applicable to each [additional/second] file) has been displayed for the first time to restrict

subsequent display of the second data assemblage (0123 "per song" indicates the method applicable to each [additional/second] file) using the first security mechanism (0120; "the trial level access permits the user is permitted to listen to the song/track once and thereafter is precluded from listening") involving the password, wherein the processor is configured to not restrict the second data assemblage that also contains user personal data (0123 "per song" indicates the method applicable to each [additional/second] file) being displayed for the first time using the first security mechanism (0120; "the trial level access permits the user is permitted to listen to the song/track once and thereafter is precluded from listening").

With respect to claim 53, the hand portable device of claim 52, wherein at least one of the first data assemblage that contains user personal data and the second data assemblage that also contains user personal data is created in the device (0079 and drawing reference 2001).

With respect to claim 54, the hand portable device of claim 33, wherein the first security mechanism comprises a data attribute (0122; e.g. "songs/tracks are stored with certificates and are ready for sales..." and 0126; e.g. "the trial key that is preferable attached to the content") associated with the data (0037; e.g. content), said data attribute indicative of whether the data (0037; e.g. content) has been displayed for the first time, and wherein the processor is configured access control means is arranged to restrict subsequent display (0120, 0127) of the data (0037; e.g. content) by changing

the data attribute (0120, 0127) so as to require entry of the password at the input which comprises a user input means (0092, drawing reference 900).

With respect to claim 55, the hand portable device of claim 60, wherein:

the user input means comprises a user input, the memory means comprises a memory, the display means comprises a display and the access control means comprises a processor (0086 and 0130 describes a device with such components).

With respect to claim 56, the memory of claim 46, the actions further comprising:

e) displaying for a first time (0126; e.g. a "trial play" i.e. single use) in the hand portable device a second data assemblage (0123 "per song" indicates the method applicable to each [additional/second] file) of the plurality of first data assemblages that contain the user personal data (0037; e.g. "...system and method that sends data such as documents, email, music files, XML content, etc. (hereinafter "content)) without regard to the first security mechanism, and responsive to the displaying for the first time (0126; e.g. a "trial play" i.e. single use) the second data assemblage (0123 "per song" indicates the method applicable to each [additional/second] file) automatically changing the data attribute of the second data assemblage from the first type to the second type; and

f) in response to changing the data attribute of step e), automatically restricting further display (0120, 0127) of the second data assemblage using the first security

mechanism (0120; "the trial level access permits the user is permitted to listen to the song/track once and thereafter is precluded from listening").

With respect to claim 57, the memory of claim 56, the actions further comprising, before step a):

wirelessly receiving the first data assemblage at the hand portable device (0045) and before step e), wirelessly receiving the second data assemblage at the hand portable device (0098).

With respect to claim 60, A hand-portable device comprising:

user input means for user input of a password (0092, drawing reference 900);

memory means (0068) for storing data (0037; content);

display means for displaying the data (0037; content); and

access control means (0086) automatically discriminate (0046; e.g. therein it is described that encrypted content in a wrapper is acted upon for content control) between at least one defined type of data assemblages that contain user personal data (0116; wherein emails and music formats represent personal data) and other types of data assemblages that do not contain user personal data (0100: e.g. browser content; 0104: e.g. downloaded applets; 0119: e.g. notifying messages) has been displayed for a first time (0095, 0126; e.g. a single view or "trial play") at the display means and automatically responsive to detecting that the data (0037; content) has been displayed for the first time (0126; e.g. a "trial play" i.e. single use) to restrict subsequent display of

the data of the data assemblage that contains user personal data (0037; content) using a first security mechanism involving the password (0120; e.g. "...is precluded from listening without again obtaining the proper authorization." and 0138), wherein the access control means does not restrict the data being displayed for the first time using the password (0120; "the trial level access permits the user is permitted to listen to the song/track once and thereafter is precluded from listening").

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5, 8, 36, 39, and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meffert in view of Marmigere et al (U.S. Patent Application 2004/0030906), hereinafter 'Marmigere.

With respect to claim 5 and similar claims 36 and 58, Meffert does not appear to explicitly disclose where a data assemblage that contains user personal data comprises one of a short message service message or a multimedia message service message.

Marmigere, however, discloses where a data assemblage that contains user personal data comprises one of a short message service message or a multimedia message service message (0015) for protecting SMS messages.

Accordingly, in the same field of endeavor, (i.e. content protection, encryption, and messaging systems), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because Marmigere would have given Meffert further types of data to protect for the benefit of giving the system a wider range of capabilities. Furthermore, in the field of protecting user defined content (e.g. messages) in mobile devices such as cell phones (Meffert, 0130), Meffert could have used Marmigere's system to allow users to transmit SMS messages with user specified protection for the benefit of giving senders assurance that such content remains protected on a recipient's device in the event of theft (a need addressed by Meffert, 0037).

Claims 36 and 58 contain essentially the same subject matter as claim 5 and therefore is rejected with the same rationale.

With respect to claim 8, Meffert teaches The method as claimed in claim 5, where a data assemblage that contains user personal data further comprises one of an instant messaging history, a picture file; an audio file; a video file; or a collection of bookmarks (0037).

With respect to claim 39, Meffert teaches A hand-portable device as claimed in claim 36, where a data assemblage that contains user personal data further comprises one of an instant messaging history, a picture file; an audio file; a video file; and a collection of bookmarks (0037).

Claims 7, 38, and 59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meffert as applied to claims , 3, 5-6, 8-9, 20, 23, 33-37, 39-40, 46, and 52-58 and 60 above, and further in view of Schoch et al (Schoch hereafter) who filed U.S. Patent 6,460,140.

With respect to claim 7 and similar claims 38 and 59, Although Meffert teaches use of a password (e.g. 0128), they do not appear to expressly disclose a user specification of a password for use in the first security mechanism.

Schoch, however, teaches a user specification of a password (col. 3 line 61-67) for user chosen password to unlock data.

Accordingly, In the same field of endeavor, (i.e. content licensing), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because the user chose password (i.e. a user specified password) of Schoch would have given the user of Meffert further control over their content in accordance with their (sender's) wishes (see Meffert, 0046). Furthermore, such a need for a user specified password is apparent in

Meffert (e.g. 0046, 0049) to give the user control when disseminating and proliferating the content.

Claims 38 and 59 contain essentially the same subject matter and therefore are rejected with the same rationale.

Claims 61-64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meffert in view of Kanai et al. (U.S. Patent 7,072,983), hereinafter 'Kanai'.

With respect to claim 61, Meffert teaches the method of claim 20, where each of said data assemblages is comprised of at least one file (0037) and automatically discriminating (0046; e.g. therein it is described that encrypted content in a wrapper is acted upon for content control) but does not expressly teach where automatically discriminating is based on file content determined using a multipurpose internet mail extension (MIME).

Kanai, however, teaches automatically discriminating is based on file content determined using a multipurpose internet mail extension (MIME) (col. 7 lines 13-15 and lines 40-43) for detecting MIME file types.

Accordingly, in the same field of endeavor, (i.e. messaging services), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because the system of Meffert, which can handle any contend that is in electronic form (Meffert, 0024), could have used the MIME type detection as taught by Kanai for the benefit of efficiently

determining which files or content may be protected or wrapped and thus which files need special processing. Furthermore, Kanai would have given Meffert extensible definitions to files (e.g. emails) for the benefit of enhanced message transmissions.

With respect to claim 62, Meffert teaches The hand-portable device of claim 33, where each of said data assemblages is comprised of at least one file (0037), and where said processor is configured to automatically discriminate (0046; e.g. therein it is described that encrypted content in a wrapper is acted upon for content control) between the at least one defined type of data assemblages that contain user personal data (0116; wherein emails and music formats represent personal data) and the other types of data assemblages that do not contain user personal data (0100: e.g. browser content; 0104: e.g. downloaded applets; 0119: e.g. notifying messages).

Meffert does not appear to expressly teach automatically discriminating based on file content determined using a multipurpose internet mail extension (MIME).

Kanai, however, teaches automatically discriminating based on file content determined using a multipurpose internet mail extension (MIME) (col. 7 lines 13-15 and lines 40-43) for detecting MIME file types.

Accordingly, in the same field of endeavor, (i.e. messaging services), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because the system of Meffert, which can handle any contend that is in electronic form (Meffert, 0024), could have used the MIME type detection as taught by Kanai for the benefit of efficiently

determining which files or content may be protected or wrapped and thus which files need special processing. Furthermore, Kanai would have given Meffert extensible definitions to files (e.g. emails) for the benefit of enhanced message transmissions.

With respect to claim 63, Meffert teaches The memory of claim 46, where each of said data assemblages is comprised of at least one file (0037) and automatically discriminating (0046; e.g. therein it is described that encrypted content in a wrapper is acted upon for content control) but does not expressly teach where automatically discriminating is based on file content determined using a multipurpose internet mail extension (MIME).

Kanai, however, teaches automatically discriminating is based on file content determined using a multipurpose internet mail extension (MIME) (col. 7 lines 13-15 and lines 40-43) for detecting MIME file types.

Accordingly, in the same field of endeavor, (i.e. messaging services), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because the system of Meffert, which can handle any contend that is in electronic form (Meffert, 0024), could have used the MIME type detection as taught by Kanai for the benefit of efficiently determining which files or content may be protected or wrapped and thus which files need special processing. Furthermore, Kanai would have given Meffert extensible definitions to files (e.g. emails) for the benefit of enhanced message transmissions.

With respect to claim 64, Meffert teaches the hand-portable device of claim 60, where each of said data assemblages is comprised of at least one file (0037), and where said access control means is configured to automatically discriminate (0046; e.g. therein it is described that encrypted content in a wrapper is acted upon for content control) between the at least one defined type of data assemblages that contain user personal data (0116; wherein emails and music formats represent personal data) and the other types of data assemblages that do not contain user personal data (0100: e.g. browser content; 0104: e.g. downloaded applets; 0119: e.g. notifying messages).

Meffert does not appear to expressly teach automatically discriminating based on file content determined using a multipurpose internet mail extension (MIME).

Kanai, however, teaches automatically discriminating based on file content determined using a multipurpose internet mail extension (MIME) (col. 7 lines 13-15 and lines 40-43) for detecting MIME file types.

Accordingly, in the same field of endeavor, (i.e. messaging services), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because the system of Meffert, which can handle any contend that is in electronic form (Meffert, 0024), could have used the MIME type detection as taught by Kanai for the benefit of efficiently determining which files or content may be protected or wrapped and thus which files need special processing. Furthermore, Kanai would have given Meffert extensible definitions to files (e.g. emails) for the benefit of enhanced message transmissions.

Response to Arguments

Applicant's arguments (see response filed 3/16/2009) with respect to the pending claims have been considered but are not found persuasive.

Applicant argues on page 12 of the response that Meffert does not anticipate or suggest automatically discriminating between at least one defined type of data assemblages that contain user personal data and other types of data assemblages that do not contain user personal data" and/or "storing at least one data attribute for each of a plurality of first data assemblages that contain the user personal data...."

Examiner disagrees and asserts that Meffert teaches the argued limitation as addressed above. Specifically, Meffert teaches automatically discriminating (0046; e.g. therein it is described that encrypted content in a wrapper is acted upon for content control) between at least one defined type of data assemblages that contain user personal data (0116; wherein emails and music files represent personal data) and other types of data assemblages that do not contain user personal data (0100: e.g. browser content; 0104: e.g. downloaded applets; 0119: e.g. notifying messages).

Moreover, Examiner submits that Meffert suggests such discrimination by applying one time (i.e. claimed "first view") restrictions to personal data such as emails (e.g. Meffert, 0079, 0095 and figure 4A). Examiner submits that the emails in Meffert may be seen as user personal data at least because an email can be seen as personal. In other words, an email is addressed to a single person and thus is seen as *personal*. Furthermore, other types of data such as bills and statements (Meffert, 0116) can be seen as user personal.

Furthermore, the music files as taught by Meffert to be authorized under a single use (Meffert, 0126) may be seen as user personal data as well. That is, the files streamed to a user and downloaded on their device teaches *user personal data*. In another way, the downloaded music is personal in that the data is unlocked for and owned by the user (Meffert, 0126). Moreover, the music files in Meffert may be seen as user personal in that the present invention describes such files as user personal data (e.g. see presently pending dependant claim 8).

As described above, Meffert is respectively seen to teach the type of data assemblages that contain user personal data. As such, because Meffert's system is seen to effect protection for only these types of data (Meffert, 0079, 0126), the argued limitation of "automatically discriminating" is found unpersuasive. In other words, Meffert protects the types of data with single view and trial play attributes. On the other hand, Meffert is seen to freely process other types (e.g. types of data assemblages that do not contain user personal data) of data such as browser content that may pass to and from the Internet (0100), downloaded applets (0109) and notifying messages (0119).

Examiner submits that because Meffert protects certain types of data and other types may not be protected, that Meffert teaches the claimed discrimination of types of data.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent 6,119,014 to Alperovich et al. The subject matter therein pertains to the pending claims (i.e. SMS protection).

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ROBERT TIMBLIN whose telephone number is (571)272-5627. The examiner can normally be reached on M-Th 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John R. Cottingham can be reached on 571-272-7079. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ROBERT TIMBLIN/
Examiner, Art Unit 2167

/John R. Cottingham/
Supervisory Patent Examiner, Art Unit 2167